Navigating in the Cayley graphs of $\mathrm{SL}_N(\mathbb{Z})$ and $\mathrm{SL}_N(\mathbb{F}_p)$

Albany Group Theory Conference
9th October 2004

Tim Riley

The Fibonacci numbers:

$$F_0 = 0, \quad F_1 = 1$$

$$F_{i+2} = F_{i+1} + F_i$$

For $i \neq j$ define e_{ij} to be the matrix in $\mathrm{SL}_N(\mathbb{Z})$ with entry ij and all diagonal entries 1 and all other entries 0.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{e_{23}{}^{2}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{e_{23}{}^2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{23}e_{32})^n} \begin{pmatrix} 1 & 0 & 0 \\ 0 & F_{2n+1} & F_{2n+3} \\ 0 & F_{2n} & F_{2n+2} \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{e_{23}{}^2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{23}e_{32})^n} \begin{pmatrix} 1 & 0 & 0 \\ 0 & F_{2n+1} & F_{2n+3} \\ 0 & F_{2n} & F_{2n+2} \end{pmatrix}$$

$$\xrightarrow{e_{13}} \begin{pmatrix} 1 & F_{2n} & F_{2n+2} \\ 0 & F_{2n+1} & F_{2n+3} \\ 0 & F_{2n} & F_{2n+2} \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{e_{23}{}^2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{23}e_{32})^n} \begin{pmatrix} 1 & 0 & 0 \\ 0 & F_{2n+1} & F_{2n+3} \\ 0 & F_{2n} & F_{2n+2} \end{pmatrix}$$

$$\xrightarrow{e_{13}} \begin{pmatrix} 1 & F_{2n} & F_{2n+2} \\ 0 & F_{2n+1} & F_{2n+3} \\ 0 & F_{2n} & F_{2n+2} \end{pmatrix} \xrightarrow{(e_{23}e_{32})^{-n}} \begin{pmatrix} 1 & F_{2n} & F_{2n+2} \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{e_{23}{}^{2}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{23}e_{32})^{n}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & F_{2n+1} & F_{2n+3} \\ 0 & F_{2n} & F_{2n+2} \end{pmatrix}$$

$$\xrightarrow{e_{13}} \begin{pmatrix} 1 & F_{2n} & F_{2n+2} \\ 0 & F_{2n+1} & F_{2n+3} \\ 0 & F_{2n} & F_{2n+2} \end{pmatrix} \xrightarrow{(e_{23}e_{32})^{-n}} \begin{pmatrix} 1 & F_{2n} & F_{2n+2} \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{e_{23}{}^{-1}} \begin{pmatrix} 1 & F_{2n} & F_{2n+2} \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{e_{23}{}^{2}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{23}e_{32})^{n}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & F_{2n+1} & F_{2n+3} \\ 0 & F_{2n} & F_{2n+2} \end{pmatrix}$$

$$\xrightarrow{e_{13}} \begin{pmatrix} 1 & F_{2n} & F_{2n+2} \\ 0 & F_{2n+1} & F_{2n+3} \\ 0 & F_{2n} & F_{2n+2} \end{pmatrix} \xrightarrow{(e_{23}e_{32})^{-n}} \begin{pmatrix} 1 & F_{2n} & F_{2n+2} \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{e_{23}{}^{-1}} \begin{pmatrix} 1 & F_{2n} & F_{2n+2} \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{23}e_{32})^{n}} \begin{pmatrix} 1 & F_{2n} & F_{2n+2} \\ 0 & F_{2n+1} & F_{2n+2} \\ 0 & F_{2n} & F_{2n+1} \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{e_{23}^{\,2}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{23}e_{32})^n} \begin{pmatrix} 1 & 0 & 0 \\ 0 & F_{2n+1} & F_{2n+3} \\ 0 & F_{2n} & F_{2n+2} \end{pmatrix}$$

$$\xrightarrow{e_{13}} \begin{pmatrix} 1 & F_{2n} & F_{2n+2} \\ 0 & F_{2n+1} & F_{2n+3} \\ 0 & F_{2n} & F_{2n+2} \end{pmatrix} \xrightarrow{(e_{23}e_{32})^{-n}} \begin{pmatrix} 1 & F_{2n} & F_{2n+2} \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{e_{23}^{\,-1}} \begin{pmatrix} 1 & F_{2n} & F_{2n+2} \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{23}e_{32})^n} \begin{pmatrix} 1 & F_{2n} & F_{2n+2} \\ 0 & F_{2n+1} & F_{2n+2} \\ 0 & F_{2n} & F_{2n+1} \end{pmatrix}$$

$$\xrightarrow{e_{13}^{\,-1}} \begin{pmatrix} 1 & 0 & F_{2n} \\ 0 & F_{2n+1} & F_{2n+2} \\ 0 & F_{2n} & F_{2n+1} \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{e_{23}{}^{2}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{23}e_{32})^{n}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & F_{2n+1} & F_{2n+3} \\ 0 & F_{2n} & F_{2n+2} \end{pmatrix}$$

$$\xrightarrow{e_{13}} \begin{pmatrix} 1 & F_{2n} & F_{2n+2} \\ 0 & F_{2n+1} & F_{2n+3} \\ 0 & F_{2n} & F_{2n+2} \end{pmatrix} \xrightarrow{(e_{23}e_{32})^{-n}} \begin{pmatrix} 1 & F_{2n} & F_{2n+2} \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{e_{23}{}^{-1}} \begin{pmatrix} 1 & F_{2n} & F_{2n+2} \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{23}e_{32})^{n}} \begin{pmatrix} 1 & F_{2n} & F_{2n+2} \\ 0 & F_{2n+1} & F_{2n+2} \\ 0 & F_{2n} & F_{2n+1} \end{pmatrix}$$

$$\xrightarrow{e_{13}{}^{-1}} \begin{pmatrix} 1 & 0 & F_{2n} \\ 0 & F_{2n+1} & F_{2n+2} \\ 0 & F_{2n} & F_{2n+1} \end{pmatrix} \xrightarrow{(e_{23}e_{32})^{-n}} \begin{pmatrix} 1 & 0 & F_{2n} \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{e_{23}{}^{2}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{23}e_{32})^{n}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & F_{2n+1} & F_{2n+3} \\ 0 & F_{2n} & F_{2n+2} \end{pmatrix}$$

$$\xrightarrow{e_{13}} \begin{pmatrix} 1 & F_{2n} & F_{2n+2} \\ 0 & F_{2n+1} & F_{2n+3} \\ 0 & F_{2n} & F_{2n+2} \end{pmatrix} \xrightarrow{(e_{23}e_{32})^{-n}} \begin{pmatrix} 1 & F_{2n} & F_{2n+2} \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{e_{23}{}^{-1}} \begin{pmatrix} 1 & F_{2n} & F_{2n+2} \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{23}e_{32})^{n}} \begin{pmatrix} 1 & F_{2n} & F_{2n+2} \\ 0 & F_{2n+1} & F_{2n+2} \\ 0 & F_{2n} & F_{2n+1} \end{pmatrix}$$

$$\xrightarrow{e_{13}{}^{-1}} \begin{pmatrix} 1 & 0 & F_{2n} \\ 0 & F_{2n+1} & F_{2n+2} \\ 0 & F_{2n} & F_{2n+1} \end{pmatrix} \xrightarrow{(e_{23}e_{32})^{-n}} \begin{pmatrix} 1 & 0 & F_{2n} \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{e_{23}{}^{-1}} \begin{pmatrix} 1 & 0 & F_{2n} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Lemma. *For* $n \geq 0$, *the words*

$$e_{23}{}^{-1}(e_{23}e_{32})^{-n}e_{13}{}^{-1}(e_{23}e_{32})^{n}e_{23}{}^{-1}(e_{23}e_{32})^{-n}e_{13}(e_{23}e_{32})^{n}e_{23}{}^{2},$$

and

$$e_{23}{}^{-1}(e_{23}e_{32})^{-n}e_{12}{}^{-1}(e_{23}e_{32})^{n}e_{23}{}^{-1}(e_{23}e_{32})^{-n}e_{12}(e_{23}e_{32})^{n}e_{23}{}^{2}$$

equal $e_{13}{}^{F_{2n}}$ *and* $e_{13}{}^{F_{2n+1}}$, *respectively, in* $\mathrm{SL}_3(\mathbb{Z})$.

Zeckendorf's Theorem. *Every positive integer m can be expressed as*

$$m = F_{k_1} + F_{k_2} + \cdots + F_{k_r},$$

with $k_1 \geq 2$ and $k_{j+1} - k_j \geq 2$ for all $1 \leq j < r$.

Proposition. *There exists $C > 0$ such that for all $N, m, i, j \in \mathbb{Z}$ such that $N \geq 3$, $1 \leq i, j \leq N$, and $i \neq j$, we can find a word w_m on $\left\{e_{pq}^{\pm 1} \mid p \neq q\right\}$ with $w_m = e_{ij}^{\,m}$ in $\mathrm{SL}_N(\mathbb{Z})$ and*

$$\ell(w) \leq C + C \log(1 + |m|).$$

Lemma. *Suppose m is a positive integer expressed as per Zeckendorf. Write*

$$m = (F_{\hat{k}_1} + F_{\hat{k}_2} + \cdots + F_{\hat{k}_{\hat{r}}}) + (F_{\bar{k}_1} + F_{\bar{k}_2} + \cdots + F_{\bar{k}_{\bar{r}}})$$

where $\hat{k}_1 < \ldots < \hat{k}_{\hat{r}}$ are the even numbers amongst $k_1, \ldots, k_r$ and $\bar{k}_1 < \ldots < \bar{k}_{\bar{r}}$ are the odd numbers. Let n be the integer such that either $2n = k_r$ or $2n + 1 = k_r$. Let u_m be the word

$$a_n b_n (e_{23} e_{32}) \ldots a_2 b_2 (e_{23} e_{32}) a_1 b_1 (e_{23} e_{32})$$

in which $a_i = e_{13}$ if $2i \in \{\hat{k}_1, \ldots, \hat{k}_{\hat{r}}\}$ and is the empty string otherwise, and $b_i = e_{12}$ if $2i + 1 \in \{\bar{k}_1, \ldots, \bar{k}_{\bar{r}}\}$ and is the empty string otherwise. Let v_m be the word obtained from u_m by replacing every e_{12} and e_{13} by ${e_{12}}^{-1}$ and ${e_{13}}^{-1}$, respectively. Define

$$w_m := {e_{23}}^{-1} (e_{23} e_{32})^{-n} v_m {e_{23}}^{-1} (e_{23} e_{32})^{-n} u_m {e_{23}}^2.$$

Then w_m equals ${e_{13}}^m$ in $\mathrm{SL}_3(\mathbb{Z})$ and has length

$$\ell(w_m) \leq 4 + 6 \log_\tau (1 + m\sqrt{5}).$$

The subtractive version of Euclid's algorithm

Example 1. Find $\gcd(-32, 8, -12) = 4$ in 6 steps:

$$\begin{aligned}
(-32, 8, -12) &\mapsto (-20,\ 8, -12) \\
&\mapsto (-8, 8, -12) \\
&\mapsto (-8, 8, -4) \\
&\mapsto (0, 8, -4) \\
&\mapsto (0, 4, -4) \\
&\mapsto (0, 0, -4).
\end{aligned}$$

Example 2. Find $\gcd(1, m) = 1$ in m steps

$$\begin{aligned}
(1, m) &\mapsto (1, m-1) \\
&\mapsto (1, m-2) \\
&\mapsto (1, m-3) \\
&\ldots \\
&\mapsto (1, 1) \\
&\mapsto (1, 0).
\end{aligned}$$

Theorem. (A.C.Yao & D.E.Knuth) *The* ***average*** *number of steps to compute* $\gcd(m, n)$ *by the (deterministic) subtractive version of Euclid's algorithm, where m is uniformly distributed in the range* $1 \leq m \leq n$*, is*

$$6\pi^{-2}(\ln n)^2 + O(\log n(\log n \log n)^2).$$

Theorem. (A.C.Yao & D.E.Knuth) *The* ***average*** *number of steps to compute* $\gcd(m, n)$ *by the (deterministic) subtractive version of Euclid's algorithm, where m is uniformly distributed in the range* $1 \leq m \leq n$*, is*

$$6\pi^{-2}(\ln n)^2 + O(\log n(\log n \log n)^2).$$

Theorem. *The* ***worst–case non–deterministic*** *complexity of the subtractive Euclid's algorithm for computing the* gcd *of* $N \geq 3$ *integers* $(a_1, \ldots, a_N)$ *is*

$$O(\log n),$$

where $n := \max\{|a_1|, \ldots, |a_N|\}$.

The Mozes–Lubotzky–Raghunathan Theorem

Theorem. *Fix $N \geq 3$. Fix a finite generating set $\mathcal{A}$ for $\mathrm{SL}_N(Z)$. There exist $C_1, C_2 > 0$ such that for all $\mathcal{M} \in \mathrm{SL}_N(\mathbb{Z})$*

$$C_1 \log \|\mathcal{M}\| \leq \ell_{\mathcal{A}}(\mathcal{M}) \leq C_2 \log \|\mathcal{M}\|.$$

Moreover, if $\mathcal{A} = \left\{e_{ij} \mid i \neq j\right\}$ then C_1 is independent of N and $C_2 \leq C_3 N^N$ for a constant $C_3 > 0$ that is independent of N.

Notation.

- $\ell_{\mathcal{A}}(\mathcal{M})$ = word length w.r.t. $\mathcal{A}$,
- $\|\mathcal{M}\|$ = max. of the absolute values of the entries.

Proof that $\ell_{\mathcal{A}}(\mathcal{M}) \leq C_3 N^N \log \|\mathcal{M}\|$.

Reduce $\mathcal{M}$ to the identity matrix using row operations:

1. Run the **accelerated version** of the subtractive Euclid's algorithm on the columns to get a matrix of the form
$$\begin{pmatrix} \pm 1 & * & * & \cdots & * \\ & \pm 1 & * & \ddots & * \\ & & \pm 1 & \ddots & \vdots \\ & & & \ddots & * \\ & & & & \pm 1 \end{pmatrix}.$$
2. Make all the entries on the diagonal 1 by premultipling by matrices $(e_{ij} e_{ji}{}^{-1} e_{ij})^2$.
3. Clear the columns using **compressed** forms of powers of e_{ij}.

Remark. The proof amounts to an algorithm that finds a *normal form* $w_{\mathcal{M}}$ of *linearly bounded length* for matrices $\mathcal{M} \in \mathrm{SL}_N(\mathbb{Z})$:

$$\ell(w_{\mathcal{M}}) \;\leq\; C_3 N^N \log \|\mathcal{M}\| \;\leq\; \frac{C_3 N^N}{C_1} \ell_{\mathcal{A}}(\mathcal{M}),$$

and so yields an "efficient means of navigating" in $\mathrm{SL}_N(\mathbb{Z})$.

Similar constructive methods yield –

Theorem. $\exists C_1 > 0, \forall N \geq 3$ *and* $\forall$ *primes* p,

$$\text{Diam } Cay\left(\text{SL}_N(\mathbb{F}_p), \left\{e_{ij} \mid i \neq j\right\}\right) \leq C_1 N^2 \ln p.$$

and an algorithm for finding paths within this bound.

Similar constructive methods yield –

Theorem. $\exists C_1 > 0, \forall N \geq 3$ *and* $\forall$ *primes* p,

$$\text{Diam } Cay\left(\text{SL}_N(\mathbb{F}_p), \left\{e_{ij} \mid i \neq j\right\}\right) \leq C_1 N^2 \ln p.$$

and an algorithm for finding paths within this bound.

Compare:

$\text{SL}_N(\mathbb{Z})$ enjoys Property (T) for $N \geq 3$.
So for a fixed $N \geq 3$ and generating set $\mathcal{A}$ for $\text{SL}_N(\mathbb{Z})$,

$$\{Cay(\text{SL}_N(\mathbb{Z}/n\mathbb{Z}), \mathcal{A}) \mid n \in \mathbb{N}\}$$

is a family of expanders. So $\exists K > 0$, such that for all primes p,

$$\text{Diam } Cay(\text{SL}_N(\mathbb{F}_p), \mathcal{A}) \leq K \log p.$$

Lemma. Every e_{ij} equals a word in $\mathcal{A}_N^{\pm 1}$ and $\mathcal{B}_N^{\pm 1}$ of length at most $13N^2$, where

$$\mathcal{A}_N := \begin{pmatrix} 1 & 1 & & & \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}, \quad \mathcal{B}_N := \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & 0 & \ddots & \\ & & & \ddots & 1 \\ (-1)^{N-1} & & & & 0 \end{pmatrix}.$$

Corollary. *There exists $C_2 > 0$ such that for all $N \geq 3$ and primes p,*

$$\text{Diam } Cay(\text{SL}_N(\mathbb{F}_p), \{\mathcal{A}_N, \mathcal{B}_N\}) \leq C_2 N^4 \ln p.$$

Problem. (Lubotzky). Can the N^4 be improved to N^2. Such a result would be best possible because $\left|\text{SL}_N(\mathbb{F}_p)\right| \sim p^{N^2-1}$.

Fix $N \geq 3$.

Problem. Does $\mathrm{SL}_N(\mathbb{Z})$ enjoy uniform Property (T)?

Problem. (*The Independence Problem for* $\mathrm{SL}_N(\mathbb{Z})$.) Is

$$\{\, Cay(\mathrm{SL}_N(\mathbb{Z})/H, X) \mid [\mathrm{SL}_N(\mathbb{Z}) : H] < \infty,\ \langle X \rangle = \mathrm{SL}_N(\mathbb{Z}) \,\}$$

a family of expanders?

Problem. Does there exist $K > 0$ such that for all generating sets X for $\mathrm{SL}_N(\mathbb{Z})$ and all primes p

$$\mathrm{Diam}\, Cay(\mathrm{SL}_N(\mathbb{F}_p), X) \ \leq\ K \log p \ \ ?$$

Problem. Give an elementary proof of the result of Gromov that $\mathrm{SL}_3(\mathbb{Z})$ admits an exponential Dehn function.

Problem. Prove the assertion of Thurston that $\mathrm{SL}_N(\mathbb{Z})$ admits a quadratic isoperimetric function for all $N \geq 4$.